

**AFFIDAVIT OF JASON J. DEFREITAS IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Jason J. DeFreitas, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security (DHS) United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) assigned to the Boston Field Office and have been employed by HSI since 2006. I am currently assigned to the Cyber Group. Prior to my assignment to the Boston Field Office, I was assigned to the HSI Los Angeles Field Office, where I served as a member of the Intellectual Property Rights Group. In connection with my official duties, I have investigated and assisted other agents in investigating cases involving a wide variety of criminal violations including, but not limited to, fraud, intellectual property rights, cultural property theft, and child pornography. Prior to my employment with ICE HSI, I served as a United States Customs and Border Protection (CBP) officer at the Los Angeles International Airport for approximately four years. My duties included the interception and examination of individuals and merchandise for violations of United States laws.
2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure to search the residence located at 23 4<sup>th</sup> Street, Apt. 2, Attleboro, Massachusetts 02703 (the "SUBJECT PREMISES") and the person of Garry Francis BIENVENUE (YOB: 1962), as more fully described in Attachment A, which is incorporated herein by reference.
3. As described herein, there is probable cause to believe that the SUBJECT PREMISES and the person of BIENVENUE contain contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A (receipt and possession of child pornography), 18

U.S.C. § 1470 (transfer of obscene material to minors), and 18 U.S.C. § 2251(a) (attempted sexual exploitation of children) (the SUBJECT OFFENSES), which items are more specifically described in Attachment B, which is also incorporated herein by reference.

4. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES are presently located at the SUBJECT PREMISES.

#### **STATEMENT OF PROBABLE CAUSE**

5. In March 2019, the mothers of two minor-aged children, hereinafter referred to as “MINOR A” (YOB 2008) and “MINOR B” (YOB 2007) reported inappropriate text messages to the Hanover County Sheriff’s Office (“HCSO”) in Virginia between their children and the user of the Snapchat<sup>1</sup> account “gwelcome.”<sup>2</sup>
6. I have reviewed reports from HCSO. According to the reports, MINOR A’s mother observed a text message conversation between MINOR A and a friend when she was reviewing MINOR A’s cellular telephone. In the conversation, MINOR A told her friend

---

<sup>1</sup> Snapchat is a multimedia mobile application developed by Snap Inc. that allows users to share messages (consisting of images, videos, and text) with each other. One of its principle features is that pictures and messages are usually only available for a short period of time before they become inaccessible to their recipients.

<sup>2</sup> For ease of reference, the user of the **gwelcome** Snapchat account will be referred herein as “gwelcome.”

that she was “weirded out” from a text conversation she had on Snapchat with **gwelcome** and sent a screenshot of the exchange. During this Snapchat conversation, **gwelcome** told MINOR A that he knew her friend, MINOR B. In the same conversation, **gwelcome** asked MINOR A if she liked to have “sexual fun.”

7. Upon discovering the text message indicating that **gwelcome** knew MINOR B, MINOR A’s mother contacted MINOR B’s mother and notified her of the situation, which prompted both parents to go to HCSO to report the incident.
8. According to the HCSO reports, the parents of both MINOR A and MINOR B provided HCSO investigators permission to search the children’s phones. HCSO investigators reviewed the contents of both phones and determined that both MINOR A and MINOR B had been communicating with **gwelcome**. Furthermore, HCSO investigators were able to locate the conversation between **gwelcome** and MINOR A referenced above, and determined that it occurred on February 12, 2019.
9. HCSO investigators were also able to observe a chat thread between MINOR B and **gwelcome** where a non-pornographic picture of MINOR B was sent to her by **gwelcome**.<sup>3</sup>
10. In the course of its investigation, HCSO interviewed MINOR B, who was 11 years old at the time. During the interview, MINOR B stated that she had sent one or two images of her body to **gwelcome** and had received a picture from **gwelcome** of his body.
11. In April 2019, HCSO executed search warrants on the **gwelcome** Snapchat account and those belonging to MINOR A and MINOR B. I have reviewed the Snapchat returns.

---

<sup>3</sup> From this, I infer that MINOR B had first sent a picture of herself to **gwelcome**.

12. Within the contents of the **gwelcome** account, I was able to locate the conversation with MINOR A that occurred on or about February 12, 2019 and is referenced above. Excerpts of that conversation are as follows:

gwelcome: *“Hey”*

MINOR A: *“Hey”*

MINOR A: *“Who are you”*

gwelcome: *“I know your friend [MINOR B]”*

gwelcome: *“And she had on her page to add you so I did”*

MINOR A: *“Can you send me a pic of u”*

gwelcome: *“I really don’t like doing that do you like to have fun”*

MINOR A: *“I think a lot of people like to have fun”*

MINOR A: *“wym”*<sup>4</sup>

gwelcome: *“sexual fun”*

MINOR A: *“Uh why r u asking me this”*

MINOR A: *“How old r u”*

gwelcome: *“I guess that’s answer is no”*

MINOR A: *“How old r u”*

gwelcome: *“if you asking then it matters”*

MINOR A: *“Yes it does matter how old u r”*

gwelcome: *“Okay then I will remove you sorry to have bothered...”*

13. I was also able to locate a Snapchat message sent on January 17, 2019, from **gwelcome** to MINOR B within the warrant returns for both **gwelcome**’s and MINOR B’s accounts. This

---

<sup>4</sup> I understand that “wym” is frequently used as an abbreviation for “what do you mean.”

message consisted of a picture of MINOR B with dog ears and nose superimposed on MINOR B's face that appeared to have been taken with the aid of a special effect filter.<sup>5</sup> In the message, **gwelcome** texted the word, "Beautiful."

14. In reviewing the contents of the **gwelcome** account, I observed communication between **gwelcome** and the user "mahmix" on January 13, 2019. In this exchange, **gwelcome** texted, "*Or even you*" to "mahmix," and approximately 49 minutes later, "mahmix" sent an image to **gwelcome** that I believe constitutes child pornography.<sup>6</sup> This image depicts a prepubescent girl who appears to be approximately 4-6 years old, lying on her back. The child's legs are spread apart, exposing the child's vagina. The child's face cannot clearly be seen in this image.<sup>7</sup>
15. In reviewing the contents of the **gwelcome** account, I also observed several chat conversations between **gwelcome** and approximately four users who, based on pictures they sent to **gwelcome**, appear to be minor females. In the course of his communication with these users, **gwelcome** asked three of them to send pictures of themselves to him and at times told them that they were beautiful. In some of these conversations, **gwelcome**

---

<sup>5</sup> I know from my training and experience and from review of online resources that Snapchat offers a variety of "filters" that users may apply to images or videos that they send to others, including one that places dog ears and nose over the photograph subject's face.

<sup>6</sup> Photos or videos taken exchanged between users of Snapchat are referred to as "snaps." According to Snap Inc.'s ("Snap") law enforcement guide, I know that the company's servers are designed to automatically delete snaps after they have been viewed by all intended recipients, and unopened snaps are automatically deleted after 30 days. Furthermore, I know that the company's servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat setting. Unopened one-to-one chats are automatically deleted in 30 days.

<sup>7</sup> This image is available for the Court's review.

asked the users if they would watch him “play” and told one user that “*Seeing you definitely made me cum.*”

16. In one of these chat conversations, which occurred between January 13 and 20, 2019, **gwelcome** asked the user, “*You want to have fun together*” and “*Will you watch me play;*” asked the user to video call him; told her “*I am horny;*” asked the user to send pictures of herself; and, when the user sent **gwelcome** several non-pornographic images depicting a girl who appears to be approximately 12 – 14 years old, sent a message stating, “*talking and seeing to you I’m getting hard,*” and, later, “*Help me cum.*”
17. In another chat conversation with a different user, which occurred between February 12, 2019 to March 1, 2019, **gwelcome** asked, “*Can you watch me play*” followed by “*You know what I mean right*” and “*Are you alone.*” The user responded to **gwelcome** that she was not alone and was with her dad. Further along in the conversation, **gwelcome** asked, “*You want to see me cum*” and “*Send me more if you want to see more.*” In a response, this user sent **gwelcome** several non-pornographic images of herself, which show a minor female child who appears to be between the ages of 10 and 13 years old. Shortly after receiving the photos **gwelcome** asked, “*Did you see me cum*” and the user responded, “*Yeah.*” Also, in the conversation with this user, **gwelcome** stated that, “*See I’m hard*” and asked the user to video call him. Shortly thereafter, **gwelcome** asked, “*Did you see me cum*” and the user responded, “*Yes.*”<sup>8</sup>

---

<sup>8</sup> Later in this conversation it appears that another individual was using this user account and sent **gwelcome** a message demanding that he stop communicating with this user as she was only 11 years old and threatening to report him to law enforcement if he continued. This individual also told **gwelcome** that they had saved everything he had sent the child. Law enforcement has not yet identified this user.

18. Included in the warrant return was subscriber information for the **gwelcome** account, which included the following:

Account ID: gwelcome  
Email Address: gbowler47@gmail.com  
Account Creation: October 31, 2013  
Phone Number: (508) 332-2606

19. On or about April 22, 2019, HSCO issued an administrative summons to Google directing the company to produce subscriber information for the email account gbowler47@gmail.com. On or about May 20, 2019, Google responded and provided the following subscriber information:

Google Account: 758064648435  
Name: Garry Bienvenue  
Created on: May 7, 2010  
SMS: (508) 332-2606

20. HCSO determined that the telephone number associated with both the **gwelcome** Snapchat account and the gbowler47@gmail.com email account was assigned to T-Mobile. On or about May 6, 2019, HCSO issued an administrative summons to T-Mobile directing the company to produce subscriber information for the telephone number (508) 332-2606. On or about May 17, 2019, T-Mobile responded and provided the following information:

Subscriber Name: Garry F. Bienvenue  
Subscriber Address: 23 4<sup>th</sup> St., Attleboro, Massachusetts 02703  
Status: Active  
Activation Date: July 4, 2008  
Account #: 576305892

21. A review of records held by the Massachusetts Registry of Motor Vehicles (“RMV”) showed that Garry Francis BIENVENUE<sup>9</sup> (YOB: 1962) is assigned a Massachusetts driver’s license, which includes the SUBJECT PREMISES as his residential address. RMV records also indicate that BIENVENUE has a 2009 gray Ford Fusion, assigned Massachusetts registration 4896 HT, registered to him at the SUBJECT PREMISES.
22. In or about May 2019, HCSO investigators contacted Taunton Police Department (“TPD”) Detective Randy DeMello and referred this matter to him as member of the Massachusetts Internet Crimes Against Children Task Force (“ICAC”) once it was suspected that BIENVENUE was the user of the **gwelcome** account. Over the course of several months, Detective DeMello received information and evidence developed from the HSCO investigation into this matter. Once a complete review of that information and evidence was conducted, this investigation was referred to HSI Boston.
23. In the course of conducting surveillance in February 2020, Detective DeMello observed BIENVENUE’s vehicle parked directly in front of the SUBJECT PREMISES, and observed that one of the mailboxes at the SUBJECT PREMISES had a label affixed to it listing the address for the SUBJECT PREMISES and the names, “Michon / Bienvenue.” RMV records indicate that Ruth M. Michon (YOB: 1949) also lists 23 4<sup>th</sup> St., Attleboro, Massachusetts 02703 as her residential address.

#### **Characteristics Common to Individuals who Consume Child Pornography**

24. Based on my previous investigative experience related to child pornography investigations,

---

<sup>9</sup> I know that “bienvenue” is French for “welcome.” Considering this, the **gwelcome** username is consistent with the first letter of BIENVENUE’s first name and the English translation of his surname.



and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web-based services to access with intent to view and possess, collect, receive, or distribute images of child pornography (*i.e.*, consumers of child pornography), as follows:

- a. Consumers of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media.
- b. Consumers of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, videos, books, drawings, other visual media, and, increasingly, digital format. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Consumers of child pornography almost always possess and maintain their child pornographic material (whether stored in hard copy or digitally) in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, videos, digital media, and other documentation of child pornography and child erotica for many years.<sup>10</sup>

---

<sup>10</sup> See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections).

Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

- d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and other digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.<sup>11</sup>
- e. Consumers of child pornography also may correspond with and/or meet others to share information and materials; often maintain correspondence from other child pornography consumers; conceal such correspondence as they do their sexually explicit material; and often maintain the contact information of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Consumers of child pornography prefer not to be without access to child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

25. Based upon all of the foregoing, I believe that BIENVENUE is the user of the **gwelcome**

---

<sup>11</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

Snapchat account and, thus, is a consumer of child pornography who has actively sought to have minor girls produce and distribute child pornography. Therefore, I submit that it is likely that he possesses some of these characteristics common to consumers of child pornography.

### **Search and Seizure of Computer Systems and Data**

26. As set forth above, probable cause exists to believe that the federal offenses described above were perpetrated through the use of computer equipment capable of accessing the internet.
27. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:
  - a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.
  - b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
  - c. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how the computer

has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.

- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

28. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media (“computer equipment”) be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

- a. The volume of evidence — storage media such as hard disks, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names.

Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

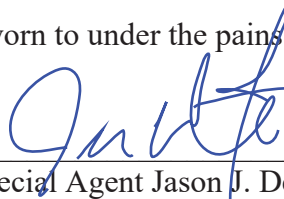
- b. Technical requirements — analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”
- 29. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.
  - 30. The SUBJECT PREMISES may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive

determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine its true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

### CONCLUSION

31. Based on all of the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A (receipt and possession of child pornography), 18 U.S.C. § 1470 (transfer of obscene material to minors), and 18 U.S.C. § 2251(a) (attempted sexual exploitation of children), as described in Attachment B, are located at the SUBJECT PREMISES, and on the person of Garry Francis BIENVENUE, as more fully described in Attachment A.

Sworn to under the pains and penalties of perjury,




Special Agent Jason J. DeFreitas  
Homeland Security Investigations

Subscribed and sworn to before me this 11th day of March, 2020

  
Honorable Jennifer C. Boal  
United States Magistrate Judge

I have reviewed the image referenced in Paragraph 14 above and I find probable cause to believe that it depicts a minor engaged in sexually explicit conduct. The affiant shall preserve the image provided to the Court for the duration of the pendency of this matter, including any relevant appeal process.

  
Honorable Jennifer C. Boal  
United States Magistrate Judge